UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

BARI VAPNEK
5535 North Military Trail
Boca Raton, Florida 33496,

On behalf of herself and all others similarly situated,

v.

MARRIOTT INTERNATIONAL INC. (a Montgomery County, Maryland Resident)
10400 Fernwood Road
Bethesda, Maryland 20817

CASE NO.: 1:18-cv-03889

CLASS ACTION

JURY TRIAL DEMANDED

Plaintiff Bari Vapnek brings this Class Action Complaint against Marriott International, Inc. ("Marriott" or "Defendant") on behalf of herself and all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

SUMMARY OF THE ALLEGATIONS

1. Marriott is a leading global lodging company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 billion in the fiscal year 2017. *See* About Marriott International – Find Your World, https://www.marriott.com/marriott/aboutmarriott.mi (last visited Dec. 17, 2018).

2. Marriott also operates and franchises hotels and licenses vacation ownership resorts.

3. In 2016, Marriott acquired Starwood Hotels & Resorts ("SPG'), creating the world's largest hotel company. Starwood hotel brands include W Hotels, St. Regis, Sheraton

Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels.

4. To book reservations for an SPG property, customers are required to provide Marriott with "Personally Identifiable Information" or "PII," which can include a combination of: guest names, addresses (both postal and email), credit card information and/or debit card and/or payment information, date and place of birth, nationality, passport, visa, or other government-issued identification data, travel itinerary, social media account information. PII can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

5. On November 30, 2018, Marriott announced that a breach of the company's Starwood computer network resulted in hackers obtaining access to over 500 million accounts, and all of the information accessible in and through those accounts (the "Data Breach").

6. Plaintiff brings this class action against Marriott for its failure to secure its customers' PII.

PARTIES

7. Plaintiff Bari Vapnek is a resident and citizen of Florida. Plaintiff has stayed at SPG properties numerous times since 2014 and provided Marriott with PII during the time that hackers had access to the SPG reservation information. After the Data Breach was announced by Marriott, Plaintiff received an email notification informing her that her information was included in the SPG database and that she is therefore affected by the Data Breach.

8. Defendant Marriott maintains its headquarters in Bethesda, Maryland. Marriott conducts its business throughout Maryland, the nation, and internationally.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over the state law claims pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the amount in controversy exceeds $5,000,000 exclusive of interests and costs, there are more than 100 class members, and

at least one class member is a citizens of a state different from that of Defendant. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391 as Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Defendant's headquarters are located within this District. A substantial part of the acts or omissions at issue in this action occurred in this District. Marriott expects Maryland law to apply to disputes with customers and to be sued in Maryland: its Terms of Use, which Marriott says applies to customers using Marriott sites, including SPG websites, shall be construed and enforced under the laws of the State of Maryland.[1] In addition, Marriott's Terms of Use state that consumers agree and submit to the jurisdiction of the State and Federal Courts situated in the State of Maryland.

FACTUAL BACKGROUND

A. Marriott Collected And Stored Detailed and Massive Amounts Of PII

11. According to Marriott's Global Privacy Statement, Marriott collects data "through websites operated by us from which you are accessing this Privacy statement," "through the software applications made available by use for use on or through computers and mobile devices," "through our social media pages that we control from which you are accessing this Privacy statement," "through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us," and "when you visit or stay as a guest at one of our properties, or through other offline interactions." https://www.marriott.com/about/privacy.mi

12. The PII Marriott collects include:

(a) Name

(b) Gender

(c) Postal address

[1] *See* https://www.marriott.com/about/terms-of-use.mi (last visited Dec. 17, 2018).

(d) Telephone Number

(e) Email address

(f) Credit Card and debit card number or other payment data

(g) Financial information in limited circumstances

(h) Language preference

(i) Date and place of birth

(j) Nationality, passport, visa, or other government-issued identification data

(k) Important dates, such as birthdays, anniversaries and special occasions

(l) Membership or loyalty program data

(m) Employer details

(n) Travel itinerary, tour group or activity data

(o) Prior guest stays or interactions, goods and services purchased, special service and amenity requests

(p) Geolocation information

(q) Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts.[2]

B. Marriott Commits To Implement Reasonable and Effective PII Security Practices

13. Marriott maintains that it seeks "to use reasonable organizational, technical and administrative measures to protect personal data." *Id.*

14. Customers place value in data privacy and security, and they consider it when making decisions regarding their online behavior. Plaintiff would not have provided the same types and amounts of PII to Marriott had she known that Marriott does not take reasonable and necessary precautions to secure the information.

---

[2] Marriott Group Global Privacy Statement, https://www.marriott.com/about/privacy.mi (last visited Dec. 17, 2018). Marriott's collection of personal data additionally, in limited circumstances, may include: data about family members and companions, biometric data, images, video, audio data, guest preferences, and personal data. *Id.*

15. Marriott failed to maintain reasonable and adequate data security, thereby allowing the Data Breach affecting at least 500 million customers worldwide.

16. Numerous hacks targeting consumers' PII have put Marriott on notice that identity thieves target PII and that hackers will go to great lengths to attain PII. Recent large-sale data breaches have targeted PII held by Equifax, Yahoo, Anthem, Premera, Target, and many other companies. According to Statista, there were 169 million records exposed in 2015 – more than double the number exposed in 2014 (85,610,000), many of them pertaining to the compromise of PII.[3] Indeed, as alleged below, SPG suffered a data breach in 2015.

C. Marriott's Inadequate Security Practices Permitted Attackers To Breach 500 Million Guest Accounts

17. According to Marriott, on September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott thereafter engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that it was from the Starwood guest reservation database.

18. The information copied from the Starwood guest reservation database over time includes PII for guests who made a reservation at a Starwood property, including names, mailing addresses, phone numbers, email addresses, passport numbers, SPG information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, as well as other PII identified in Marriott's Privacy Policy, discussed above.

19. The combination of PII varies by guest. For some individuals, the information copied included, *inter alia*, payment card numbers and payment card expiration dates. Although the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-

[3] Statista, https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide (last visited Dec. 17, 2018).

128), Marriott has stated that it has not been able to rule out the possibility that the encryption has been defeated.

20. On November 30, 2018, Marriott disclosed to the public that a breach of the company's Starwood computer network (described above and herein) resulted in hackers obtaining direct access to over 500 million customer accounts, and all of the information accessible in and through those accounts.

21. For approximately 327 million guests, the PII breached includes a combination of name, mailing address, phone number, email address, passport number, SPG account information, date of birth, gender, communication preference, and payment card number and payment card expiration date.

22. The Data Breach occurred because of Marriott's unreasonable and inadequate data security practices, as is evidenced by the fact that Marriott failed to even discover the breach for over 4 years. Indeed, as reported by the *Wall Street Journal* on December 2018, in an article titled "*Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*," Marriott failed to conduct a thorough investigation into a smaller 2015 breach at SPG that, had it been done right, could have uncovered the Data Breach:

> Marriott International Inc. MAR -5.04% says it responded quickly when it learned in recent weeks of a colossal theft of customer data. But cybersecurity specialists say the company missed a significant chance to halt the breach years earlier.
> Marriott on Friday said the hack of the reservation database for its Starwood properties, which involved the theft of personal information on up to 500 million customers, began in 2014 and went undetected until this September.
>
> In 2015, Starwood reported a much smaller breach, in which attackers installed malware on point-of-sale systems in some hotel restaurants and gift shops to siphon off payment-card information. It disclosed the attack four days after Marriott announced a deal to acquire Starwood Hotels & Resorts Worldwide for what ended up being $13.6 billion, creating the No. 1 hotel company globally.
>
> Marriott says that the 2015 incident was different and not related to the attack made public Friday. But security specialists say that while it's not unusual for breach investigations to miss a second intruder, a more thorough investigation into the 2015 intrusion could have uncovered the attackers, who instead were able to lurk in its reservation system for three more years. "With all the resources they have, they should

have been able to isolate hackers back in 2015," said Andrei Barysevich, a researcher with the security company Recorded Future Inc.

Stolen PII Is Valuable To Hackers And Thieves

23. It is well known, and the subject of many media reports, that PII data is highly coveted and a frequent target of hackers. The issue of data security and threats thereto is well known, as noted above. Despite well-publicized litigation and frequent public announcements of data breaches by some of the world's largest companies, Marriott opted to maintain an insufficient and inadequate system to protect the PII of Plaintiff and class members.

24. Legitimate organizations and the criminal underground alike recognize the value of PII. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[4] Similarly, the 2017 Equifax data breach resulted in the compromise of records containing the PII of at least 145.5 million customers in the United States and nearly 1 million customers outside of the United States.

25. Biographical data, such as the birthdate and place of birth collected by Marriott, is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[5] PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of theft and unauthorized access have been the subject of many media reports.

26. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of third parties, Marriott's approach at maintaining the privacy of Plaintiff and Class members' PII was negligent.

---

[4] Verizon 2014 PCI [Payment Card Industry] Compliance Report, https://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf , at 54 (last visited Dec. 17, 2018) ("2014 Verizon Report").

[5] 2014 Verizon Report, at 54.

D. This Data Breach Will Result In Additional Identity Theft And Identity Fraud

27. The ramifications of Marriott's failure to keep Plaintiff's and Class members' data secure are severe.

28. Identity thieves can use PII such as that of Plaintiff and Class members to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Among other forms of fraud, identity thieves may get medical services using customers' compromised PII or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

29. In fact, identity theft is one of the most common outcomes from data breaches. 31.7% of breach victims in 2016 later experienced identity fraud, compared to just 2.85% of individuals not notified of a data breach in 2016, according to Javelin Strategy & Research. *See* Identity Theft Statistics, Experian, https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

30. According to First Data's results of its 2018 Consumer Cybersecurity Study: "The results of the survey show that consumers lack awareness as to how much of their PII is on the dark web, and have little trust in businesses' abilities to keep their data safe," said EJ Jackson, Head of Security and Fraud Solutions, First Data. "Advances in technology are opening new opportunities for fraudsters to obtain PII, and businesses must proactively respond by implementing technology solutions that keep consumer data safe and secure." Press Release, First Data, First Data Releases Cybersecurity Study on PII (Oct. 17, 2018), https://investor.firstdata.com/financial-news/2018/10-17-2018-114447103.

31. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

E. Plaintiff And Class Members Suffered Damages

32. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

33. Plaintiff's and Class members' PII is private and sensitive in nature and was left inadequately protected by Marriott. Marriott did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

34. As a direct and proximate result of Marriott's wrongful action and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud.

35. Marriott's wrongful actions and inaction directly and proximately caused the theft of Plaintiff's and Class members' PII, causing them to suffer actual harm for which they are entitled to compensation, including:

(a) theft of their PII;

---

[6] GAO, *Report to Congressional Requesters*, at p.33 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Dec. 17, 2018).

(b) the imminent and certainly impending injury flowing from potential fraud and identify theft posed by the misuse of their PII;

(c) the improper disclosure of their PII;

(d) loss of privacy; and

(e) ascertainable losses in the form of the value of their PII, for which there is a well-established market.[7]

36. While the PII of Plaintiff and members of the Class has been stolen, the same or a copy of the PII continues to be held by Marriott. Plaintiff and members of the Class have an undeniable interest in ensuring that this information is secure, remains secure, and is not subject to further theft.

37. Marriott recognizes that the Data Breach has injured its customers. It has set up a website for affected consumers (at https://answers.kroll.com), offering a dedicated call center and one free year of "WebWatcher Enrollment," normally a pay service that Marriott says will "monitor[] internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found." However, even if WebWatcher is effective at mitigating the harm of identity theft, one year is a grossly inadequate time frame because the effects of identity theft linger for many years, as alleged above. Because of the Data Breach, Plaintiff and Class members face years of constant surveillance and monitoring of their financial and personal records. In addition, they will expend money to pay for WebWatcher after the inadequate 1-year free period ends, or will pay for other identity-theft protection services.

[7] *See also, e.g.*, GAO, August 2018 Data Protection Actions Taken By Equifax and Federal Agencies in Response to the 2017 Breach, https://www.gao.gov/assets/700/694158.pdf

CLASS ACTION ALLEGATIONS

38. Plaintiff seeks relief in her individual capacity and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of:

> All persons in the United States whose PII was compromised as a result of the Data Breach disclosed on November 30, 2018.

39. Excluded from each of the above Classes are Marriott, including any entity in which Marriott has a controlling interest, is a parent or subsidiary, or which is controlled by Marriott, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Marriott. Also excluded are the judges and court personnel assigned to this case.

40. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Marriott has acknowledged that the accounts of 500 million guests were affected by the breach, including Plaintiff's.

41. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

(a) Whether Marriott had a duty to reasonably secure customer PII, and whether it breached that duty;

(b) Which security procedures and which data-breach notification procedures should Marriott be required to implement as part of any injunctive relief ordered by the Court;

(c) Whether Marriott has an implied contractual obligation to use reasonable security measures;

(d) Whether Marriott has complied with any implied contractual obligation to use reasonable security measures;

(e) What security measures, if any, must be implemented by Marriott to comply with its implied contractual obligations; and

(f) What the nature of the relief should be, including equitable relief, to which Plaintiff and the Class members are entitled.

42. All members of the proposed Classes are readily ascertainable. Marriott has access to addresses and other contact information for the millions of members of the Class, which can be used for providing notice to many Class members.

43. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other class member, was inadequately safeguarded through Marriott's uniform misconduct.

44. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

45. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

46. Pursuant to Fed. R. Civ. P. 23(c)(4), Plaintiff and the class seek certification of particular claims and issues in the alternative to certification of all issues and claims.

47. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Marriott's violations of law inflicting substantial damages in the aggregate would go un-remedied.

48. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Marriott has acted or has refused to act on grounds generally applicable to the Class, so

that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Breach of Implied Contract

49. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 48.

50. Marriott solicited and invited Plaintiff and Class Members to use its reservation services. Plaintiff and Class members accepted Marriott's offers and created guest accounts requiring the provision of PII with Marriott during the period of the Data Breach.

51. When Plaintiff and Class Members used Marriott services and products, they provided their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Marriott pursuant to which Marriott agreed to safeguard and protect such information.

52. Each use of a Marriott service made by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with Marriott under which Marriott agreed to safeguard and protect Plaintiff and Class Members' PII.

53. Plaintiff and Class Members would not have provided and entrusted their PII to Marriott in the absence of the implied contract between them and Marriott.

54. Plaintiff and Class Members fully performed their obligations under the implied contracts with Marriott.

55. Marriott breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the PII of Plaintiff and Class.

56. As a direct and proximate result of Marriott's breaches of the implied contracts between Marriott and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above

COUNT II

Negligence

57. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 56.

58. Upon accepting and storing Plaintiff's and Class Members' PII in its computer network, Marriott undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Marriott knew and acknowledged that the PII was private and confidential and would be protected as private and confidential.

59. In addition to undertaking a duty by its own acts of soliciting PII from customers, Marriott owed an independent duty of care pursuant to the Maryland Personal Information Protection Act (Md. Code Ann., Com. Law § 14-3501), which requires that "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations." Md Code Ann. Com. Law § 14-3503. The PII collected by Marriott and compromised in the Data Breach is "personal information" pursuant to Md. Code Ann. Com. Law § 14-3501(e) because it included a name and some combination of "[a] Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government . . . [or] an account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account."

60. Marriott breached its duty to Plaintiff and the Class Members to adequately protect and safeguard this information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured personal PII. Marriott failed to provide adequate supervision and oversight of the PII with which it is entrusted,

in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

61. Through Marriott's acts and omissions described in this Complaint, including Marriott's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Marriott unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII during the time it was within Marriott's possession or control.

62. Upon information and belief, Marriott improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

63. Marriott's failure to take proper security measures to protect Plaintiff and Class Members' sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff and Class Members' PII.

64. Marriott's conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct adequate regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' PII.

65. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

66. As a direct and proximate cause of Marriott's conduct, Plaintiff and the Class suffered damages as alleged above.

COUNT III

Unjust Enrichment

67. Plaintiff repeats and fully incorporates the allegations contained in paragraphs 1 through 66.

68. Plaintiff and members of the Class conferred a benefit upon Marriott by entrusting Marriott with their PII in utilizing Marriott's reservation services, which benefitted Marriott.

69. Marriott accepted and retained the benefits conferred by Plaintiff and the Class members.

70. Marriott has been unlawfully enriched at the expense of Plaintiff and members of the Class by failing to secure customers' PII, and Marriott's acceptance and retention of the benefits would make it inequitable for Marriott to retain the benefit without the paying of value in return .

71. Plaintiff and members of the Class are entitled to damages as a result of Marriott's unjust enrichment, including all profits accruing to Marriott because of its unlawful and unfair business practices.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Marriott as follows:

a. For an Order certifying the Class as defined here, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Marriott from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Marriott to utilize appropriate methods and policies with respect to guest data collection, storage, and safety and to disclose with specificity to Class members the type of PII compromised.

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Marriott's wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial of her claims by jury to the extent authorized by law.

DATED: December 17, 2018

/s/ Hassan Zavareei
Hassan Zavareei

TYCKO & ZAVAREEI LLP
Hassan Zavareei (No. 18489)
1828 L Street, NW, Suite 1000
Washington, DC 20036
Telephone: (202) 417- 3658
Facsimile: (202) 973-0950

MILBERG TADLER PHILLIPS GROSSMAN LLP
Ariana J. Tadler
Henry J. Kelston
Andrei V. Rado
Jennifer Czeisler
One Pennsylvania Plaza, Suite 1920
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229